Title: Cyberatak w świetle międzynarodowego prawa humanitarnego konfliktów zbrojnych

Author: Aleksandra Kacała-Szwarczyńska

Citation style: Kacała-Szwarczyńska Aleksandra. (2019). Cyberatak w świetle międzynarodowego prawa humanitarnego konfliktów zbrojnych. "Journal of Modern Science" (2019), T. 2, s. 169–188.
DOI: 10.13166/JMS/111176

Aleksandra Kacała-Szwarczyńska
Uniwersytet Śląski w Katowicach Wydział Prawa i Administracji
olakacala@gmail.com
ORCID 0000-0002-2139-4710

DOI: 10.13166/JMS/111176
JOURNAL OF MODERN SCIENCE TOM 2/41/2019, S. 169–188

Cyberattack in the context of international humanitarian law of armed conflicts

Cyberatak w świetle międzynarodowego prawa humanitarnego konfliktów zbrojnych

Abstract

Countries are investing more and more resources in developing offensive and defensive capabilities in cyberspace. This is mainly caused by an increasing number of cyberattacks directed against both civilians and states. The subject of this article is an attempt to find a definition of a cyberattack in the existing international humanitarian law of armed conflicts, with particular emphasis on the specificity of cyberspace. The concept of cyberattack includes similarities with the concept of attack consolidated in international law. Differences in cybernetic space, however, introduce dissonance in terms of understanding the cyberattack and the possibility of applying to cyberattack existing legal norms. These factors, on the other hand, have or may have a direct or indirect impact on the security and rights of the civilians.

Streszczenie

Państwa inwestują coraz większe zasoby w rozwijanie zdolności ofensywnych i defensywnych w cyberprzestrzeni. Spowodowane jest to w głównej mierze coraz większą liczbą cyberataków skierowanych zarówno przeciwko ludności cywilnej, jak i państwom. Przedmiotem niniejszego artykułu jest próba odnalezienia definicji cyberataku w istniejącym międzynarodowym prawie humanitarnym konfliktów zbrojnych, ze szczególnym uwzględnieniem specyfiki cyberprzestrzeni. Poję-

cie cyberataku zawiera punkty styczne z utrwalonym w prawie międzynarodowym pojęciem ataku. Odmienności przestrzeni cybernetycznej wprowadzają jednak dysonans w zakresie rozumienia samego pojęcia cyberataku, jak też możliwości stosowania do niego istniejących norm prawnych. Powyższe czynniki natomiast mają lub mogą mieć przełożenie bezpośrednio lub pośrednio na bezpieczeństwo i prawa ludności cywilnej.

Keywords: *cyberattack, law, armed conflicts, technology, cyberspace*

Słowa kluczowe: *cyberatak, prawo, konflikty zbrojne, technologia, cyberprzestrzeń*

Wprowadzenie

W związku z rozwojem technologii państwa oraz podmioty niepaństwowe coraz częściej obok lub zamiast dotychczasowych metod prowadzenia konfliktów zbrojnych wykorzystują cyberatak. Wobec licznych działań podejmowanych w cyberprzestrzeni, przedstawiciele doktryny, w przeciwieństwie do państw[1], nie mają raczej wątpliwości, że prawo konfliktów zbrojnych powinno stosować się również do cyberataków (Schimitt M., Vihul L., 2014, s. 43). Spory, które pojawiają się w tym przedmiocie, dotyczą raczej sposobu stosowania prawa konfliktów zbrojnych do cyberataku.

Społeczność międzynarodowa nie zawarła do tej pory umowy międzynarodowej, która regulowałaby w sposób kompleksowy konflikty w cyberprzestrzeni. Rozwijane jest natomiast *soft law*, które dzięki swojej elastyczności znakomicie wypełnia lukę w prawie międzynarodowym publicznym, sprzyja procesom kodyfikacji oraz kształtowaniu się prawa zwyczajowego.

Tak zwane *miękkie prawo* dotyczące prawa konfliktów zbrojnych w cyberprzestrzeni jest rozwijane m.in. przez *NATO Cooperative Cyber Defence Centre of Excellence*. Pod auspicjami organizacji opracowano podręczniki dotyczące prawa międzynarodowego cybernetycznych konfliktów zbrojnych, tj. *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt M., 2013) oraz *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Schmitt M., 2017) (dalej jako: „Tallinn Manual"). Tallinn Manual zawiera zestawienie norm prawa międzynarodowego dotyczących cyberoperacji opatrzone komentarzem wybitnych przedstawicieli doktryny.

Celem niniejszego artykułu jest analiza cyberataku na podstawie źródeł międzynarodowego prawa humanitarnego konfliktów zbrojnych (dalej jako:

MPH) i Tallinn Manual oraz wyodrębnienie węzłowych problemów wynikających z zaangażowania cyberprzestrzeni w konflikty zbrojne. Niezależnie zostanie podjęta próba sporządzenia postulatów *de lege ferenda*.

Charakterystyka cyberataku

Niniejsze rozważania w dużej mierze zostaną oparte na kryterium porównawczym cyberataku do ataku z wykorzystaniem klasycznych środków zbrojnych. Podobnie jak w prawie kosmicznym, analogia może wpłynąć korzystnie na rozwój prawa cyberprzestrzeni. Prawo międzynarodowe publiczne jest niezwykle bogate i służy wielu zróżnicowanym przestrzeniom (Schmitt M., 2017), nie wydaje się zatem zasadne, aby cyberprzestrzeń stanowiła w tym zakresie wyjątek. Uwzględnić należy oczywiście charakterystykę i odmienność cyberprzestrzeni, a w konsekwencji również cyberataku.

Zgodnie z zasadą 92 Tallinn Manual cyberatak można zdefiniować jako defensywną lub ofensywną cyberoperację, która powoduje rany, śmierć osób lub zniszczenie mienia. Jednocześnie wskazuje się, że bez znaczenia pozostaje kwestia czy konflikt jest międzynarodowy czy nie (Bielecki D.M., 2010, s. 415). Powyższe pozostaje spójne z art. 49 ust. 1 Protokołu dodatkowego do konwencji genewskich z 12 sierpnia 1949 r. dotyczących ochrony ofiar międzynarodowych konfliktów zbrojnych (dalej jako: Protokół Dodatkowy), zgodnie z którym określenie „atak" oznacza akt przemocy w stosunku do przeciwnika, zarówno zaczepny, jak i obronny. Zatem istotą ataku i cyberataku jest przemoc, co oznacza, że z pojęcia cyberataku należy wykluczyć cyberszpiegostwo oraz działania psychologiczne stosowane za pośrednictwem cyberprzestrzeni (Federal Ministry of Defence of the Federal Republic of Germany 1992).

Powyższe nie oznacza, że atakiem jest wyłącznie działanie kinetyczne. Przykładowo zgodnie ze stanowiskiem Międzynarodowego Trybunału Karnego dla byłej Jugosławii przez atak należy rozumieć m.in. użycie broni chemicznej, biologicznej czy radiologicznej, które nie zawsze mają przecież charakter kinetyczny (Wyrok Międzynarodowego Trybunału Karnego dla byłej Jugosławii, 1995). Analogicznie, w przypadku cyberataku to konsekwencje działań w cyberprzestrzeni mogą determinować, czy dana operacja stanowi atak w rozumieniu MPH (Schmitt M., 2017, s. 416–419).

Stosowanie MPH nie powinno zostać ograniczone wyłącznie do *klasycznych* metod prowadzenia walki. Artykuł 35 Protokołu Dodatkowego wskazuje, że dobór metod walki jest ograniczony w tym sensie, że nie powinno się stosować metod walki powodujących zbędne cierpienie oraz rozległe, długotrwałe i poważne szkody dla środowiska. Jeśli zatem cyberatak nie wywoła skutków, o których mowa w zdaniu poprzedzającym, ta metoda walki będzie dopuszczalna. Celem tych regulacji jest bowiem ochrona osób i dóbr przed skutkami konfliktów zbrojnych, a nie wyłączenie określonych metod prowadzenia działań zbrojnych (Gąska M., Ciupiński A., 2001, s. 22). W konsekwencji uzasadnione jest przyjęcie, że podstawowe zasady MPH znajdują zastosowanie w cyberoperacjach. Jednocześnie legalność nowych broni powinna być każdorazowo weryfikowana na podstawie norm MPH (Janusz-Pawletta B., 2013, s. 112–113).

Jednocześnie wciąż aktualna wobec cyberataku pozostaje ochrona urządzeń zawierających tzw. niebezpieczne siły takie jak zapory, groble czy elektrownie jądrowe. Nie mogą być one przedmiotem cyberataku, nawet jeżeli stanowią cel wojskowy. Nie jest to jednak ochrona bezwzględna, ponieważ może ustać, w przypadku gdy obiekty te są używane do celów odmiennych niż ich przeznaczenie lub jeśli dostarczają wsparcia operacjom wojskowym i atak na nie jest jedynym możliwym środkiem do spowodowania ustania takiego wsparcia. Należy jednak wówczas przedsięwziąć wszelkie dostępne środki ostrożności dla uniknięcia wyzwolenia niebezpiecznych sił (Janusz-Pawletta B., 2013, s. 115–116).

Cyberatak skierowany przeciwko ludności cywilnej, kombatantom oraz nielegalnym kombatantom

Międzynarodowe prawo zwyczajowe nakazuje, aby w toku stosowania działań zbrojnych przestrzegać podstawowych zasad prawa humanitarnego, w tym w szczególności zasady proporcjonalności, rozróżnienia, humanitaryzmu i konieczności wojskowej (Schmitt M., 2017, s. 83). Stosowanie zasad MPH nie jest uzależnione od sposobu prowadzenia walk, co oznacza, że reguły te powinny znajdować zastosowanie również w przypadku cyberataku.

Cyberatak powinien być ściśle ograniczony do celów wojskowych. Określenie *cel wojskowy* używane jest jako całościowy plan danej operacji lub w węższym znaczeniu jako konkretny cel, tj. osoba lub obiekt (Marcinko M., 2014, s. 132–133). Ludność cywilna nie powinna być oczywiście celem cyberataku, lecz przeciwnie – korzysta z ogólnej ochrony przed niebezpieczeństwami wynikającymi z operacji wojskowych.

W przypadku wątpliwości co do statusu danej osoby należy ją traktować jako ludność cywilną (Schmitt M., 2017, s. 424). Doktryna angielska stoi na stanowisku, zgodnie z którym wyłącznie *istotne* wątpliwości dotyczące przynależności danej osoby do ludności cywilnej, istniejące pomimo uzyskania informacji ze wszystkich dostępnych w danym czasie źródeł uzasadniają zastosowanie powyższego domniemania (UK Ministry of Defence, 2004 par. 5.3.4). W opozycji do *istotnych wątpliwości* w orzecznictwie Międzynarodowego Trybunału Karnego pojawia się termin *uzasadnionych wątpliwości* (Wyrok Międzynarodowego Trybunału Karnego dla byłej Jugosławii, 2003 par. 55). Oba twierdzenia doprowadzają do konkluzji, że wątpliwości natury ogólnej nie są wystarczające do zastosowania ekstensywnie ochrony prawnej (Schmitt M., 2017, s. 424–425).

MPH nakazuje, aby podczas operacji wojskowych stale podejmować działania ochronne wobec ludności cywilnej i podjąć wszelkie dostępne środki ostrożności, które umożliwią jej ochronę. Istniejące obecnie rozwiązania technologiczne umożliwiają prowadzenie stosunkowo szczegółowych czynności rozpoznawczych i sprawdzających. Nie sposób jednak zawsze zidentyfikować statusu użytkownika sieci internetowej, co wzmaga trudności w stosowaniu zasady rozróżniania w przypadku cyberataku.

MPH obok ludności cywilnej wyróżnia legalnych uczestników działań zbrojnych, czyli kombatantów oraz niekombatantów, którzy jednak z uwagi na podejmowane czynności bojowe korzystają ze statusu analogicznego/podobnego do kombatantów (Janusz-Pawletta B., 2013, s. 46), a także nielegalnych kombatantów podlegających odpowiedzialności na gruncie MPH i potencjalnie odpowiedzialności karnej za nielegalny udział w działaniach zbrojnych (Łubieński P., 2009, s. 43).

Status jednostki zależy od stopnia i charakteru zaangażowania takiej osoby w działania militarne. Cyberatak może zostać skierowany zasadniczo

przeciwko członkom sił zbrojnych, członkom zorganizowanych grup militarnych, ludności cywilnej, jeśli i tak długo jak uczestniczy bezpośrednio w starciach oraz w przypadku międzynarodowych konfliktów zbrojnych – przeciwko uczestnikom pospolitego ruszenia (*levée en masse*) (Łubieński P., 2009, 425).

Członków sił zbrojnych należy zdefiniować jako osoby, które są członkami zasadniczych sił państwowych, w tym *in statu nascendi* (Sandoz Y., Swinarski Ch., Zimmermann B., 1986, par. 1621–2622) z wyłączeniem personelu sanitarnego, duchowieństwa wojskowego, chorych i rannych (Konwencja o polepszeniu losu rannych i chorych w armiach czynnych, 1949). Jednocześnie członkowie sił zbrojnych niebędący kombatantami, jak np. doradcy prawni, których zadania nie obejmują uczestnictwa w działaniach zbrojnych, mogą stanowić cel cyberataku, gdyż ze względu na przynależność do sił zbrojnych tracą status osoby cywilnej, a w razie dostania się do niewoli uzyskują status jeńca wojennego (Janusz-Pawletta B., 2013 s. 46, 52). Stosowanie wobec tej grupy cyberataku wydaje się uzasadnione koniecznością wojskową, a jej zakres i natężenie będzie determinowany przez rozwój technologiczny państwa lub grupy sojuszników.

Przez zorganizowaną grupę militarną można rozumieć oddziały ochotnicze, w tym ruch oporu, który posiada struktury i jest zdolny do prowadzenia działań wojskowych (Schmitt M., 2017, s. 389), jeśli posiada osobę odpowiedzialną za podwładnych, znak rozpoznawczy, jawnie nosi broń i przestrzega praw i zwyczajów wojennych (w rozumieniu I Konwencji Genewskiej z 12 sierpnia 1949 r.) lub przynajmniej odróżnia się od ludności cywilnej (w rozumieniu Protokołu Dodatkowego) (Janusz-Pawletta B., 2013, s. 50). Sporne w doktrynie jest to, czy samo członkostwo w zorganizowanej grupie militarnej uprawnia drugą stronę konfliktu do zastosowania wobec danej osoby cyberataku. Ze względu na militarny charakter grupy militarnej i jej cel funkcjonowania można argumentować, że konieczność wojskowa uzasadnia stosowanie cyberataku do takich osób nawet wyłącznie po uwzględnieniu kryterium przynależności. Natomiast jeżeli struktura wojskowa składa się zarówno ze skrzydła militarnego, jak i politycznego, to wyłącznie część militarna powinna być kwalifikowana jako zorganizowana grupa militarna (Schmitt M., 2017, s. 426), co pozostaje spójne z podsta-

wowymi zasadami prawa humanitarnego. Nieregularne siły zbrojne tracą w konfliktach niemiędzynarodowych status kombatanta, a co za tym idzie, mogą zostać pociągnięte do odpowiedzialności karnej już za sam udział w walce. Podmioty takie określa się najczęściej mianem rebeliantów czy *unlawful combatant* (Janusz-Pawletta B., 2013, s. 53).

Zagadnienie ludności cywilnej, która uczestniczy bezpośrednio w starciach, budzi istotne trudności wyodrębnienia takiej grupy w praktyce. Zgodnie z przepisami MPH status tych osób różni się zarówno od rebeliantów, jak i ruchu oporu. Niezorganizowane i spontaniczne wzięcie udziału w walkach powoduje, że osoba cywilna traci swój status ochronny, ale wyłącznie na czas walki. Po zakończeniu spontanicznych działań jednostkę należy traktować jako osobę cywilną (*hors de combat)* (Melzer N., 2009, par. 1621–1622). Osoba uczestnicząca bezpośrednio w starciach nie posiada statusu kombatanta, a tym samym nie chroni jej w tym zakresie MPH. Może zostać zatem pociągnięcia do odpowiedzialności karnej i międzynarodowej na gruncie MPH za nielegalny udział w walkach. Określenie *bezpośredni udział w działaniach zbrojnych* niesie wiele wątpliwości interpretacyjnych. Zgodnie z wykładnią rozszerzającą, bezpośredni udział w działaniach zbrojnych to również przygotowanie, wykonywanie i dowodzenie, jeżeli możliwe jest przypisanie danej osobie odpowiedzialności. W takim przypadku osoba cywilna nieprzerwanie wykonuje czynności bojowe (*continuous combat function*). W praktyce taka interpretacja może jednak doprowadzić do fikcji ochrony prawnej takich osób w okresie, gdy nie podejmują one żadnych czynności militarnych. W konsekwencji uważa się, że kryterium ciągłej funkcji bojowej negatywnie wpływa na równowagę pomiędzy zasadą konieczności wojskowej a zasadą humanitaryzmu (Góździewicz W., 2012, s. 33–45).

Ciekawym zjawiskiem jest status personelu prywatnych firm (*private military contractors*) (Kinsey Ch., 2007, s. 8–10) (dalej jako: PMC). Ich kwalifikacja do właściwej kategorii zależy od charakteru ich działań i jest wysoce dyskusyjna. Są to cywilni pracownicy świadczący usługi wspomagające lub zastępcze w celu zwiększenia efektywności działań armii lub zbrojnych grup podczas międzynarodowych i niemiędzynarodowych konfliktów zbrojnych (Kurecki Ł., 2013, s. 318). Zasadniczo rolą prywatnych podmiotów jest przejmowanie od regularnych sił zbrojnych za wynagrodzeniem niektórych zadań

na zasadzie *outsourcingu* (Gaston E.L., 2008, s. 224). Ich zadania są niezwykle zróżnicowane i zakwalifikowanie PMC do odpowiedniej grupy, tj. jako kombatantów (np. dostawcy), ludności cywilnej (pracownicy wojskowi lub milicja) czy najemników, powinno być rozpatrywane indywidualnie. PMC po spełnieniu odpowiednich przesłanek mogą występować w konfliktach. Zakwalifikowanie PMC jako kombatanta powoduje objęcie takie osoby najszerszą ochroną MPH. Określenie PMC jako ludność cywilna biorąca udział bezpośrednio w walkach lub najemników powoduje utratę przez nich m.in. immunitetu jeńca wojennego i potencjalnie naraża na odpowiedzialność karną i na podstawie MPH (Ghazi Janaby M., 2016, s. 81).

Zgodnie z art. 47 ust. 2 I Protokołu Dodatkowego najemnikiem jest osoba, która spełni łącznie sześć kumulatywnych przesłanek. Osoba taka została specjalnie zwerbowana w kraju lub za granicą do walki w konflikcie zbrojnym; rzeczywiście bierze bezpośredni udział w działaniach zbrojnych; bierze udział w działaniach zbrojnych głównie w celu uzyskania korzyści osobistej i otrzymała od strony konfliktu lub w jej imieniu obietnicę wynagrodzenia materialnego wyraźnie wyższego od tego, które jest przyrzeczone lub wypłacane kombatantom mającym podobny stopień i sprawującym podobną funkcję w siłach zbrojnych tej strony; nie jest obywatelem strony konfliktu ani stałym mieszkańcem terytorium kontrolowanego przez stronę konfliktu; nie jest członkiem sił zbrojnych strony konfliktu; nie została wysłana przez państwo inne niż strona konfliktu w misji urzędowej jako członek sił zbrojnych tego państwa. Definicja najemnika jest zredagowana w sposób zawężający tak, aby pozbawienie ochrony wynikającej ze statusu kombatanta i jeńca wojennego następowało jedynie w ściśle określonych sytuacjach i dotyczyło jak najwęższej kategorii osób (United Nations High Commissioner for Human Rights United Nations Office, 2002, s. 6).

Udział bezpośredni PMC jako ludności cywilnej w walkach jest nieuprawniony, zarówno w przypadku ich zakwalifikowania, jak i niezakwalifikowania jako najemników. PMC ścigani są wówczas za naruszenie MPH oraz jeżeli przewidują to przepisy krajowe, mogą zostać pociągnięci do odpowiedzialności karnej. W praktyce jednak pociągnięcie PMC do odpowiedzialności jest trudne. Państwo natomiast odpowiada za czyny PMC niezgodne z MPH, jeżeli można mu przypisać odpowiedzialność, co powoduje, że ostatecznie

pociągnięcie do odpowiedzialności takich podmiotów może w ogóle nie nastąpić (Janusz-Pawletta B., 2013, s. 48–50).

PMC mogą być uznani zatem za legalnych lub nielegalnych kombatantów (Kurecki Ł., 2013, s. 343–345) i stanowić cel cyberataku. Prawo do cyberataku ze względów strategicznych jest uzasadnione koniecznością wojskową zarówno w odniesieniu do dostawców, jak i najemników. Prawo do cyberataku może zostać jednak wobec nich ograniczone przy wystąpieniu odpowiednich przesłanek wyłączenie do czasu, kiedy bezpośrednio uczestniczą w walce. Przyjęcie powyższego stanowiska, z jednej strony, wydaje się zasadne, ponieważ prowadzi do ograniczenia pozytywnego prawa do stosowania cyberataku. Z drugiej strony, należy zastanowić się czy wykładnia rozszerzająca nie zachęci do podejmowania współpracy z podmiotami o niejasnym statusie prawnym będącymi w praktyce najemnikami, których działanie ma często destrukcyjny wpływ na stabilność państwa, a także określane jest jako negatywne z perspektywy pokoju i bezpieczeństwa (United Nations High Commissioner for Human Rights United Nations Office at Geneva, 2002, s. 9).

Ostatnią omawianą grupą jest *levée en masse*. Pospolite ruszenie, w odróżnieniu od ludności cywilnej uczestniczącej bezpośrednio w walkach, może być celem cyberataku, również poza okresem bezpośredniego uczestnictwa w walkach (Waters Ch., 2014). *Levée en masse* można zdefiniować jako ludność niezajętego terytorium, która wobec zbliżających się sił nieprzyjacielskich spontanicznie podejmuje walkę w celu odparcia wroga, nie mając jeszcze wykształconych struktur. Prawo międzynarodowe w I Konwencji Genewskiej przyznaje takim osobom status strony wojującej, jeśli jawnie noszą broń i przestrzegają prawa i zwyczajów wojennych (Henckaerts J.M., Doswald-Beck L., 2009, s. 18). Wobec posiadania pewnego immunitetu przynależnego kombatantom członkowie *levée en masse* są potencjalnym celem cyberataku.

Cyberatak skierowany przeciwko obiektom

Poza wprowadzeniem w art. 52 Protokołu Dodatkowego ogólnego zakazu atakowania dóbr o charakterze cywilnym, Protokół Dodatkowy nie definiuje wprost, czym są dobra o charakterze cywilnym. Dobra o charakterze cywil-

nym zostały określone jako dobra, które nie są celami wojskowymi. Celami wojskowymi są natomiast dobra, które ze swej natury, rozmieszczenia, przeznaczenia lub wykorzystania wnoszą istotny wkład do działalności wojskowej i których całkowite lub częściowe zniszczenie, zajęcie lub zneutralizowanie daje określoną korzyść w danej sytuacji. W art. 52 ust. 3 Protokołu Dodatkowego wskazano, że przykładowo dobrami o charakterze cywilnym jest miejsce kultu religijnego, dom czy szkoła.

Charakterystyka obiektów

Protokół dodatkowy został sporządzony w sześciu wersjach językowych. W wersji angielskiej, arabskiej, chińskiej i rosyjskiej stosuje się pojęcie *object*. W wersji hiszpańskiej i francuskiej wprowadzono natomiast odpowiednio pojęcie *los bienes* i *les biens,* które odpowiadają polskiej wersji językowej *dobra.* MPH nie definiuje pojęcia *obiektu* czy *dóbr*. Wspomagając się zatem wykładnią językową oraz normatywną, należy wskazać, że pojęcie *dóbr* jest dwuwymiarowe, w przeciwieństwie do *obiektu*, który można utożsamiać z *rzeczą.* Zgodnie z art. 45 Kodeksu cywilnego (dalej jako: kc) przez pojęcie *dóbr* rozumie się zarówno przedmioty materialne (przykładowo: art. 757 kc obejmujący *ratowanie dobra innej osoby* dotyczy raczej dóbr materialnych), jak i prawa niematerialne (przykładowo: art. 23 kc dotyczący dóbr osobistych).

Z Protokołu dodatkowego wprost wynika, że przez dobra o charakterze cywilnym można rozumieć rzeczy (np. miejsce kultu religijnego, dom czy szkoła). Potwierdzają to również autorzy Komentarza Międzynarodowego Czerwonego Krzyża do Protokołów Dodatkowych z 1987 r., którzy wskazują, że przez pojęcie obiektu rozumie się rzeczy widoczne i materialne (ang. *visible and tangible*). W konsekwencji należy wywieść wniosek, że struktura cybernetyczna taka jak komputery, linie światłowodowe i inne materialne przedmioty stanowią obiekty, do których stosuje się prawo konfliktów zbrojnych (Sandoz Y., Swinarski Ch., Zimmermann B., 1986, par. 2007–2008).

Grupa ekspertów opracowująca Tallin Manual nie była zgodna, czy obiekt powinien być wyłącznie bytem materialnym czy też może mieć formę niematerialną. Zgodnie z istniejącą wykładnią cyberatak wobec danych nie będzie podlegał MPH, chyba że spowoduje zaburzenie funkcjonalności struktury cybernetycznej (Schmitt M., 2017, s. 450).

Rozwój technologiczny spowodował, że dane – informacje mają niejednokrotnie wartość większą niż rzeczy. Destrukcja danych medycznych, podatkowych, bankowych narusza prawa i bezpieczeństwo ludności cywilnej – zwłaszcza jeżeli nie ma możliwości ich przywrócenia (Schmitt M., 2017, s. 437).

Przykładem dóbr niematerialnych, których objęcie ochroną postulują niektórzy przedstawiciele doktryny (m.in. H.H. Dinniss, K. Mačák w przeciwieństwie do M. Schmitt), jest budzący wiele kontrowersji kod źródłowy tworzący program komputerowy. Zwolennicy rozszerzenia pojęcia obiektu na kod źródłowy twierdzą, że w przeciwieństwie do przywracalnych danych, kod stanowi wartość operacyjną, której uszkodzenie powoduje utratę funkcjonalności i może wywołać poważne skutki dla bezpieczeństwa państwa i jego obywateli. W praktyce mogą zostać zaatakowane elektrownie, oczyszczalnie ścieków, systemy komunikacyjne czy bankowe. Przeciwnicy rozszerzenia pojęcia obiektu na kod źródłowy wskazują, że kod nie jest rzeczą, tj. nie jest widoczny i nie ma formy materialnej, a posiada jedynie odbicie w postaci zapisu – równania logicznego (Schmitt M., 2017, s. 437). Literalna i systemowa wykładnia postanowień art. 52 ust. 2 Protokołu dodatkowego wskazuje, że kod źródłowy nie jest chronionym dobrem o charakterze cywilnym. W pewnych przypadkach jednak zaatakowanie kodu źródłowego spowoduje skutki kinetyczne, które pozwolą stwierdzić, że zaatakowano (pośrednio) obiekt cywilny (np. oczyszczalnia czy trakcja kolejowa).

Innym ciekawym przykładem obiektów, których status na gruncie MPH jest niejasny, mogą być akcje zdematerializowane (Bunk J., 2017). Posiłkując się ponownie odniesieniem do prawa krajowego, należy zwrócić uwagę, że nie wszystkie akcje będą miały oprócz formy zapisu elektronicznego dokumentowy odpowiednik. W przypadku akcji zdematerializowanych *ab initio* spółka w ogóle nie wydaje dokumentów akcji (Rodzynkiewicz M., 2014). Prawa ze zdematerializowanych akcji, zgodnie z ustawą z 29 lipca 2005 r. o obrocie instrumentami finansowymi, powstają z chwilą zapisania ich po raz pierwszy na rachunku papierów wartościowych i przysługują osobie będącej posiadaczem tego rachunku. Na podstawie żądania posiadacza rachunku papierów wartościowych (akcjonariusza posiadającego akcje zdematerializowane) podmiot prowadzący rachunek papierów wartościowych wystawia posiadaczowi (akcjonariuszowi) na piśmie imienne świadectwo depozytowe.

Źródłem powstania tego prawa jest zapis elektroniczny. Akcje zdematerializowane *ab initio* wymykają się utrwalonej koncepcji materialności obiektów. Mimo że stanowią dane cyfrowe, to w przeciwieństwie do kodu źródłowego akcje posiadają jasno określoną wartość i stanowią przedmiot własności, przy czym nie są przedmiotem własności intelektualnej.

Biorąc pod uwagę powyższe, celowe wydaje się zatem rozszerzenie ochrony wynikającej z art. 52 ust. 2 Protokołu dodatkowego, jeśli nie na wszystkie dobra niematerialne, to jednak przynajmniej na określony katalog dóbr niematerialnych (Dinniss H.H., 2012). Przyjęcie progresywnej wykładni pojęcia *obiektu*, który uwzględniałby chociażby częściowo dobra niematerialne, odzwierciedlałoby poziom rozwoju technologicznego współczesnego świata i przyczyniłyby się do zwiększenia bezpieczeństwa jednostek, państwa i całej społeczności międzynarodowej. Twórcy komentarza do Protokołu dodatkowego podczas jego tworzenia w latach 80. ubiegłego wieku nie mogli przewidzieć intensywności rozwoju technologicznego i jego wpływu na bezpieczeństwo osób cywilnych. Nie stoi to jednak na przeszkodzie, aby już teraz istniejące normy Protokołu dodatkowego stosować do cyberataku, używając bardziej nowoczesnej wykładni przepisów.

Obiekt jako cel wojskowy – elementy definicyjne

Jak wskazano w art. 52 ust. 2 Protokołu dodatkowego, w odniesieniu do dóbr, celami wojskowymi są tylko takie, które z powodu swej natury, swego rozmieszczenia, przeznaczenia lub wykorzystania wnoszą istotny wkład do działalności wojskowej i których całkowite lub częściowe zniszczenie, zajęcie lub zneutralizowanie daje określoną korzyść w danej sytuacji.

Przedmiotem cyberataku nie mogą być obiekty o charakterze cywilnym lub należące do ludności cywilnej. Struktura cybernetyczna z przeznaczeniem cywilnym nie może być zatem celem cyberataku, chyba że zostanie uznana za cel wojskowy (Dinniss H.H., 2017, s. 434–435).

Zakaz atakowania obiektów cywilnych wywodzi się historycznie z deklaracji w sprawie pocisków wybuchających małego kalibru z 1868 r. Zgodnie z postanowieniami deklaracji jedynym legalnym celem, jaki państwa powinny sobie stawiać w czasie wojny, jest osłabienie sił zbrojnych nieprzyjaciela.

Reguła ta została wprowadzona również przez art. 52 ust. 1 Protokołu dodatkowego i znajduje zastosowanie zarówno do międzynarodowych, jak i niemiędzynarodowych konfliktów zbrojnych.

Obiekty cywilne nie są celem wojskowym. *A contrario* celem wojskowym mogą być wyłącznie te obiekty, które ze względu na swoją naturę, położenie, zastosowanie czy cel biorą efektywny udział w akcjach wojskowych i których całkowite lub częściowe zniszczenie, zabór lub zneutralizowanie powoduje istotną wojskową przewagę.

Struktura cybernetyczna rozumiana jako urządzenia do komunikowania się, przechowywania danych i komputery, których system został zbudowany i funkcjonuje (Schmitt M., 2017, s. 564), ze względu na swoją naturę, zastosowanie lub cel zastosowania bez wątpienia może zostać celem wojskowym (Schmitt M., 2017, s. 436–441). Pojęcie obiektu jako celu wojskowego weryfikowane jest przez pryzmat statusu (natura, położenie) lub użycia (zastosowanie, cel) obiektu (Schmitt M., 2017, 435).

Natura rzeczy obejmuje nieodłączne i charakterystyczne cechy obiektu. Oznacza to, że chodzi o obiekty typowo wojskowe i zaprojektowane do celów operacyjnych, np. komputery wojskowe (Henckaerts J.M., Doswald-Beck L., 2009, s. 32–34). W przeciwieństwie do osób, w przypadku obiektów nie funkcjonuje domniemanie, zgodnie z którym w razie wątpliwości co do statusu obiektu ma on charakter cywilny. Wskazano wyłącznie obowiązek sporządzenia jego ostrożnej weryfikacji przed zastosowaniem cyberataku (Schmitt M., 2017, s. 448).

Położenie obiektu odnosi się do powierzchni geograficznej istotnej dla celów wojskowych. Innymi słowy, to specyfika obszaru determinuje dany obiekt jako cel wojskowy, ponieważ przyczynia się do prowadzenia działalności wojskowej (Marcinko M., 2013, s. 136–137). Lokalizacją nie jest w tym kontekście adres IP. Adres IP w dużym uproszczeniu można określić jako numer nadany np. sieci komputerowej, który służy identyfikacji obiektu (Tanenbaum A., Wetherall D., 2012, s. 485). IP nie polega na używaniu przestrzeni, lecz jest związany z infrastrukturą cybernetyczną i potwierdza, że z danego obiektu wykonywane są pewne operacje. Skutki tych operacji mogą wystąpić natomiast setki kilometrów dalej od położenia sieci komputerowej (Tanenbaum A., Wetherall D., 2012, s. 438).

Przeznaczenie obiektu do celów bojowych powoduje, że staje się on celem wojskowym poprzez jego planowane przyszłe wykorzystanie (Marcinko M., 2013, s. 137–138). Przykładowo użycie sieci kolejowej, stacji telewizyjnej czy radiowej do celów wojskowych powoduje utratę ich cywilnego statusu (Henckaerts J.M., Doswald-Beck L., 2009, s. 35–36). Analogicznie traktować należy sieć komputerową należącą do osoby cywilnej. Użycie sieci w celach wojskowych powoduje utratę jej dotychczasowego charakteru i ochrony. Sieć staje się celem wojskowym, nawet jeśli ponownie wykorzystywana jest już wyłącznie przez ludność cywilną i w celach niewojskowych (Schmitt M., 2017, s. 438). Stosowanie tego kryterium powinno podlegać szczególnej ostrożności i zasadzie proporcjonalności. Uznanie sieci komputerowej za cel wojskowy nie powinno bowiem następować wówczas, gdy przykładowo tylko jeden z jej użytkowników korzysta z niej do tego celu. Fabryka, w której produkuje się części do komputerów oraz oprogramowanie, może zostać uznana za cel wojskowy, nawet jeżeli tylko część obiektów tam produkowanych będzie służyła do prowadzenia konfliktów zbrojnych. W takim przypadku należy rozważyć skalę, zakres i wkład tych czynności dla prowadzenia konfliktu zbrojnego i na tej podstawie zdecydować ostatecznie o jego kwalifikacji jako cel wojskowy lub pozawojskowy.

Przez wykorzystanie celu obiektu należy rozumieć zamierzone i oczekiwane w przyszłości zastosowanie obiektu. O celu obiektu decyduje czynnik ludzki – intencja stron. Wykazanie intencji strony przeciwnej oczywiście niesie za sobą istotne trudności dowodowe (Schmitt M., 2017, s. 438). MPH nie wprowadza szczególnych rozwiązań dotyczących uprawdopodobnienia użycia dóbr o charakterze cywilnym do celów wojskowych. Nie wprowadza również reguł wiarygodności czy źródła pozyskiwania informacji w tym przedmiocie. Od atakującego wymaga się takiego działania, którego rozsądna strona konfliktu dopuściłaby się w podobnych lub takich samych okolicznościach. Innymi słowy, należy postawić pytanie, czy rozsądnie działająca atakująca strona, procedując na podstawie racjonalnie dostępnych informacji, może stwierdzić, że dobra o charakterze cywilnym zostaną wykorzystane w celach wojskowych. Pozytywna odpowiedź na to pytanie umożliwi zakwalifikowanie obiektu jako cel wojskowy.

Infrastrukturę cybernetyczną stosowaną zarówno w celach wojskowych, jak i cywilnych należy uznać za cel wojskowy (Schmitt M., 2017, s. 439). Jednocześnie należy oczywiście pamiętać o podstawowych zasadach prawa humanitarnego takich jak proporcjonalność. Dlatego przykładowo w razie użycia portalów społecznościowych do rozszerzania informacji wojskowych, celem ataku nie powinny zostać platformy tych portali, lecz wyłącznie przedmiotowe posty.

Zakwalifikowanie obiektu jako celu wojskowego co do zasady jest możliwe, gdy obiekt spełni jedno z ww. kryteriów efektywnego udziału w akcjach wojskowych. Przedstawiciele doktryny wskazują, że przedmioty z natury służące do celów wojskowych nie muszą spełniać przesłanki efektywnego udziału w walce, aby stosowało się do nich prawo konfliktów zbrojnych (Schmitt M., 2017, s. 440). W opozycji wskazuje się, że oprócz samej natury rzeczy powinno się wykazać, czy obiekt ten jest używany w walce lub czy ją wspiera (US Department of Defence Office, 2016, par. 5.7.6.2). Za obiekt wspierający walkę można uznać m.in. systemy wydobywcze ropy naftowej, które ekonomicznie wspierają państwo będące stroną konfliktu. Powszechnie uznaje się jednak, że powyższa wykładnia jest nadmiernie rozszerzająca (Schmitt M., 2017, s. 450). Zastosowanie jej doprowadzić mogłoby do sytuacji, gdy pod pretekstem pośredniego wspierania walk przeprowadzane byłyby dowolne i nieuzasadnione koniecznością wojskową operacje.

Niezależnie należy rozważyć ostatni element normy zezwalającej na użycie cyberataku, jakim jest uzyskanie przewagi wojskowej. Celem cyberataku mogą być wyłącznie te obiekty, których zniszczenie czy zneutralizowanie ma przynieść wojskową korzyść. Zasadniczy cel operacji nie nasuwa wątpliwości. Warto zastanowić się jednak nad cyberatakami, które pośrednio mają przynieść korzyść. Uszkodzenie urządzeń lub utrudnianie łączności wojskowych komunikujących się za pomocą swoich prywatnych urządzeń z rodziną może obniżyć morale, a przesyłanie sfałszowanych informacji stanowi element wojny informacyjnej, której efektem psychologicznym ma być osłabienie strony przeciwnej. W przypadku takich działań nie zostaną jednak spełnione pozostałe przesłanki cyberataku, w tym element przemocy (Schmitt M., 2017, s. 444). W konsekwencji tego rodzaju czynności pośrednio wypływające na uzyskanie przewagi wojskowej nie mogą zostać zakwalifikowane jako cyberatak.

Podsumowanie

Państwa inwestują w coraz większe zdolności ofensywne w cyberprzestrzeni, a cyberataki skierowane przeciwko ludności cywilnej rosną. Społeczność międzynarodowa potrzebuje międzynarodowych reguł, aby chronić społeczeństwo przed zagrożeniami ze strony państw i aktorów niepaństwowych w cyberprzestrzeni. Wobec braku wypracowania wiążących norm dedykowanych cyberoperacjom na zasadzie analogii wiele zasad i przepisów MPH można stosować z powodzeniem do cyberataku. W konsekwencji należy afirmować stanowisko stosowania MPH do ochrony ludności cywilnej i dóbr o charakterze cywilnym wobec cyberataku.

W odniesieniu do stosowania MPH do cyberprzestrzeni i rozwoju technologicznego, pozytywnie należy ocenić stosowanie wykładni celowościowej. Jej bezpośrednie zastosowanie powinno dotyczyć przede wszystkim definicji dóbr o charakterze cywilnym.

Rozwój technologiczny wprowadził nowe wyzwania stanowiące praktyczne problemy i które znacznie wykraczają poza akademickie rozważania. Dane osobowe, bankowe, kody źródłowe i być może inne dobra o charakterze niematerialnym w obecnym brzmieniu przepisów i stosowanej wykładni pozostają poza ochroną art. 52 Protokołu dodatkowego. Z tego względu coraz częściej pojawiają się propozycje uchwalenia Konwencji Genewskiej związanej z technologią cyfrową[2]. Z uwagi jednak na zawrotne tempo rozwoju technologii wskazuje się, że uchwalenie powszechnie obowiązującej umowy międzynarodowej będzie trwało zbyt długo, a jej postanowienia nie nadążą za postępem technologicznym. Z tego powodu szczegółowe zagadnienia techniczne i technologiczne nie powinny stanowić przedmiotu kodyfikacji. Umowa, jeżeli taka w ogóle zostałaby utworzona, powinna być utrzymana na poziomie ogólności, który zapewni jej uniwersalny charakter. Jednocześnie powinna określać zasadnicze mechanizmy związane z cyberoperacjami oraz przedmiot, którego dotyczą. W pozostałym zakresie należy rozważyć pozostawienie cyberprzestrzeni w sferze miękkiego prawa, które jest bardziej elastyczne i dynamicznie, może przystosowywać się do nowych okoliczności. Trudność leży jednak oczywiście w stosowaniu i przestrzeganiu *soft law*.

Literatura

Bielecki, D.M., (2010). *International Humanitarian Law od armed conflict and Space Law*, [w:] Nowakowska-Małusecka J. (red.), *Międzynarodowe prawo humanitarne. Antecedencje i wyzwania współczesności*, Katowice; Bydgoszcz: Oficyna Wydawnicza Branta. ISBN 9788361668251.

Bunk, J., (2017). *The protection of intellectual property in cyberspace under international humanitarian law during cyber-operations*, referat wygłoszony na International Conference on Cyber Conflict, Estonia.

Dinniss, H.H., (2012). *Cyber warfare and the laws of war*, „Cambridge: University Press", XIX. ISBN 9781107416994.

Gąska, M., Ciupiński, A., (2001). *Międzynarodowe prawo humanitarne konfliktów zbrojnych. Wybrane problemy*, Warszawa: AON. ISBN 8388062662.

Gaston, E.L., (2008). *Mercenarism 2.0? The Rise of the Modern Private Security Industry and Its Implications for International Humanitarian Law Enforcement*, „Harvard International Law Journal", Vol. 49, No. 1. ISSN 0017-8063.

Góździewicz, W., (2012). *Bezpośredni udział ludności cywilnej w działaniach zbrojnych i jego skutki prawne*, [w:] B. Janusz-Pawletta (red.), *Ochrona ludności cywilnej przez Siły Zbrojne RP w misjach poza granicami kraju a międzynarodowe prawo humanitarne konfliktów zbrojnych*, Warszawa: AON.

Henckaerts, J.M., Doswald-Beck, L., (2009). *Customary International Humanitarian law, volum I: rules*, Cambridge: University Press. ISBN 9780521005289.

Janaby, M.G., (2016). *The legal regime applicable to private military and security company personnel in armed conflict*, Szwajcaria: Springer. ISBN 9783319422312.

Janusz-Pawletta, B., (2013). *Międzynarodowe prawo humanitarne konfliktów zbrojnych,* Warszawa: AON. ISBN 9788375232196.

Kinsey, Ch., (2007). *Corporate soldiers and international security: the rise of private military companies*, Routledge. ISBN 9780415457767.

Kurecki, Ł., (2013), *Status private military contractors w świetle międzynarodowego prawa humanitarnego,* „Międzynarodowe Prawo Humanitarne", tom IV, selektywna eliminacja i rozkaz wojskowy, Gdynia.

Łubieński, P., (2009). *Status kombatanta i ochrona jeńców wojennych*, [w:] M. Marcinko, P. Łubiński (red.), *Wybrane zagadnienia z zakresu międzynarodowego prawa humanitarnego*, Kraków: Szkoła Aspirantów Państwowej Straży Pożarnej. Centrum Szkolenia Ochrony Ludności i Dóbr Kultury. ISBN 8389877295.

Łubieński, P., (2009). *Status kombatanta i ochrona jeńców wojennych*, [w:] M. Marcinko, P. Łubiński (red.), *Wybrane zagadnienia z zakresu międzynarodowego prawa humanitarnego*, Kraków: Szkoła Aspirantów Państwowej Straży Pożarnej. Centrum Szkolenia Ochrony Ludności i Dóbr Kultury. ISBN 8389877295.

Marcinko, M., (2014). *Cele wojskowe a obiekty cywilne oraz dobra i obiekty poddane szczególnej ochronie*, [w:] Z. Falkowski, M. Marcinko (red.), *Międzynarodowe Prawo Humanitarne Konfliktów Zbrojnych*, Warszawa: Wojskowe Centrum Edukacji Obywatelskiej. ISBN 9788363755379.

Melzer, N., (2009). *Interpretive Guidance on the Notion of Direct Participation in Hostilities under IHL*, Genewa.

Rodzynkiewicz, M., (2014). *Art. 328.* [w:] M. Rodzynkiewicz (red.), *Kodeks spółek handlowych. Komentarz,* wyd. VI. Wydawnictwo Prawnicze LexisNexis. ISBN 9788327809582.

Sandoz, Y., Swinarski, Ch., Zimmermann, B. (1986). *Commentaire des Protocoles additionnels du 8 juin 1977 aux Convention de Genève du 12 aout 1949*, Genewa.

Schimitt, M., Vihul, L., (2014). *The nature of international law cyber norms*, Tallinn Paper, nr 5 Tallin.

Schmitt, M., (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press. ISBN 9781139169288.

Schmitt, M., (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press. ISBN 9781316630372.

Tanenbaum, A., Wetherall D., (2012). *Sieci komputerowe*, Gliwice: Wydawnictwo Helion. ISBN 9788324630790.

Waters, Ch., (2014), *New Hactivists and the Old Concept of Levée en Masse*, Dalhousie Law Journal, 37(2):771-786, Canada. ISSN 0317-1663.

Inne

A Digital Geneva Convention to protect cyberspace, Microsoft Policy Paper (dostęp: 13 stycznia 2018 r., https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH).

Federal Ministry of Defence of the Federal Republic of Germany humanitarian law in armed conflicts manual, 1992, par. 474, http://www.humanitaeres-voelkerrecht.de/ManualZDv15.2.pdf.

UK Ministry of Defence the joint service manual of the law of armed conflict, JSP 383, 2004,https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27874/JSP3832004Edition.pdf.

United Nations High Commissioner for Human Rights United Nations Office at Geneva, The Impact of Mercenary Activities on the Right of Peoples to Self-determination, "Human Rights Fact Sheet" 2002, No. 28.

US Department of Defence Office of the general counsel law of war manual, Washington 2016, par. 5.7.6.2. (dostęp 10 stycznia 2018 r., https://www.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190).

Źródła prawa

Deklaracja w sprawie pocisków wybuchających małego kalibru, Petersburg, 11 grudnia 1868 r., [w:] L. Gelberg, *Prawo międzynarodowe i historia dyplomatyczna. Wybór dokumentów, wstęp i opracowanie*, Warszawa 1954, t. I.

Konwencja o polepszeniu losu rannych i chorych w armiach czynnych (I konwencja genewska) z 12 sierpnia 1949 r. (Dz.U. z 1956 r. nr 38, poz. 171, załącznik).

Protokół dodatkowy do konwencji genewskich z 12 sierpnia 1949 r. dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych z 8 czerwca 1977 r. (Dz.U. z 1992 r. nr 41, poz. 175, załącznik).

Ustawa z 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 1964 r. nr 16, poz. 93).

Ustawa z 29 lipca 2005 r. o obrocie instrumentami finansowymi (tekst jedn.: Dz.U. z 2017 r. poz. 1768 z późn. zm.).

Orzecznictwo

Wyrok Międzynarodowego Trybunału Karnego dla byłej Jugosławii z 2 października 1995 r. w sprawie przeciwko Dusko Tadić, IT-94-1-T.

Wyrok Międzynarodowego Trybunału Karnego dla byłej Jugosławii z 5 grudnia 2003 r., IT-98-29.

Endnotes

[1] Zgromadzenie Ogólne ONZ wydało 30 grudnia 2015 r. rezolucję A/RES/70/237, która wyznaczała państwom członkowskim opracowanie wspólnego stanowiska, czy i w jaki sposób prawo międzynarodowe ma zastosowanie do korzystania przez państwa z technologii informacyjnych i komunikacyjnych grupy ekspertów rządowych ONZ. Zadanie realizowane w ramach grupy ekspertów rządowych ONZ zakończyło się porażką, w głównej mierze przez Kubę, która oświadczyła, że sprzeciwia się równoważności dokonywanej między złośliwym wykorzystaniem

technologii informacyjno-komunikacyjnych a koncepcją zbrojnego ataku. Doprowadziło to zakończenia prac bez utworzenia wspólnego stanowiska w sprawie.

[2] Przykładowo: Microsoft zaproponował utworzenie Digital Geneva Convention to protect cyberspace.